CLAIMS:

1. A method for anonymously indexing an electronic record system, the method comprising:

storing an asymmetric cryptographic private key under the control of a portable storage device of a registered user;

storing an anonymous public key certificate, the anonymous public key certificate being associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key;

providing the portable storage device with information for associating the registered user with the portable storage device; and

indexing within an electronic record system personal information of the registered user, whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate.

2. The method of claim 1 wherein the portable storage device is provided with human readable information for associating the registered user with the portable storage device.

3. The method of claim 1 wherein the portable storage device is provided with machine readable information for associating the registered user with the portable storage device upon presentation of the portable storage device.

4. The method of any one of claims 1 to 3 wherein the portable storage device is a smartcard.

5. The method of any one of claims 1 to 3 wherein the portable storage device is an electronic passport.

6. The method of any one of claims 1 to 5 wherein the indexing comprises associating with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer.

7. The method of any one of claims 1 to 6 wherein the anonymous public key certificate contains a personal data component.

8. The method of claim 7 wherein the personal data component comprises biometric data of the registered user.

9. The method of any one of claims 1 to 8, wherein storing of the asymmetric cryptographic private key under the control of the portable storage device comprises storing the asymmetric cryptographic private key in the portable storage device.

10. The method of any one of claims 1 to 8, wherein storing of the asymmetric cryptographic private key under the control of the portable storage device comprises storing an access code in the portable storage device allowing access to the asymmetric cryptographic private key.

11. The method of any one of claims 1 to 8, wherein storing of the asymmetric cryptographic private key under the control of the portable storage device comprises copying the asymmetric cryptographic private key into the possession of an authorised user.

12. The method of claim 11 wherein the copied asymmetric cryptographic private key in the possession of the user is caused to be deleted upon occurrence of a predetermined event.

13. The method of claim 12 wherein the predetermined event is the authorised user entering an update to the indexed personal information of the registered user.

14. The method of claim 12 wherein the predetermined event is lapsing of an authorisation period.

15. The method of any one of claims 11 to 14 wherein the authorised user is a health care professional authorised by the registered user to enter an update to the registered user's indexed personal information.

16. An anonymously indexed electronic record system comprising:

a portable storage device for a registered user, an asymmetric cryptographic private key being under the control of the portable storage device, the portable storage device being provided with information for associating the registered user with the portable storage device;

a stored anonymous public key certificate associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key,

an electronic storage indexing personal information of the registered user, whereby association of the information with the registered user is anonymously verifiable by use of the anonymous public key certificate.

17. The system of claim 16 wherein the portable storage device is provided with human readable information for associating the registered user with the portable storage device.

18. The system of claim 16 wherein the portable storage device is provided with machine readable information for associating the registered user with the portable storage device upon presentation of the portable storage device.

19. The system of any one of claims 16 to 18 wherein the portable storage device is a smartcard.

20. The system of any one of claims 16 to 18 wherein the portable storage device is an electronic passport.

21. The system of any one of claims 16 to 20 wherein the electronic storage indexes the personal information by having associated with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer.

22. The system of any one of claims 16 to 21 wherein the anonymous public key certificate contains a personal data component.

23. The system of claim 22 wherein the personal data component comprises biometric data of the registered user.

24. The system of any one of claims 16 to 23, wherein the asymmetric cryptographic private key is stored in the portable storage device.

25. The system of any one of claims 16 to 23, wherein an access code is stored in the portable storage device allowing access to the asymmetric cryptographic private key.

26. The system of any one of claims 16 to 23, wherein the asymmetric cryptographic private key can be copied with the registered user's authorisation into the possession of an authorised user.

27. The system of claim 26 wherein the copied asymmetric cryptographic private key in the possession of the user is caused to be deleted upon occurrence of a predetermined event.

28. The system of claim 27 wherein the predetermined event is the authorised user entering an update to the indexed personal information of the registered user.

29. The system of claim 27 wherein the predetermined event is lapsing of an authorisation period.

30. The system of any one of claims 26 to 29 wherein the authorised user is a health care professional authorised by the registered user to enter an update to the registered user's indexed personal information.

31. A portable storage device for a registered user of an anonymously indexed electronic record system, the portable storage device being provided with information for associating the registered user with the portable storage device, wherein an asymmetric cryptographic private key is under the control of the portable storage device, wherein an anonymous public key certificate is associated with an asymmetric cryptographic public key matching the asymmetric cryptographic private key, and wherein association of anonymously indexed personal information with the user is anonymously verifiable by use of the anonymous public key certificate.

32. The device of claim 31 wherein the portable storage device is provided with human readable information for associating the registered user with the portable storage device.

33. The device of claim 31 wherein the portable storage device is provided with machine readable information for associating the registered user with the portable storage device upon presentation of the portable storage device.

34. The device of any one of claims 31 to 33 wherein the portable storage device is a smartcard.

35. The device of any one of claims 31 to 33 wherein the portable storage device is an electronic passport.

36. The device of any one of claims 31 to 35 wherein the personal information is anonymously indexed by having associated with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer.

37. The device of any one of claims 31 to 36 wherein the anonymous public key certificate contains a personal data component.

38. The device of claim 37 wherein the personal data component comprises biometric data of the registered user.

39. The device of any one of claims 31 to 38, wherein the asymmetric cryptographic private key is stored in the portable storage device.

40. The device of any one of claims 31 to 38, wherein an access code is stored in the portable storage device allowing access to the asymmetric cryptographic private key.

41. The device of any one of claims 31 to 38, wherein the asymmetric cryptographic private key can be copied with the registered user's authorisation from the portable storage device into the possession of an authorised user.

42. The device of claim 41 wherein the copied asymmetric cryptographic private key in the possession of the user is caused to be deleted upon occurrence of a predetermined event.

43. The device of claim 42 wherein the predetermined event is the authorised user entering an update to the indexed personal information of the registered user.

44. The device of claim 42 wherein the predetermined event is lapsing of an authorisation period.

45. The device of any one of claims 41 to 44 wherein the authorised user is a health care professional authorised by the registered user to enter an update to the registered user's indexed personal information.

46. An electronic storage for an anonymously indexed electronic record system, the electronic storage indexing personal information of a registered user, wherein association of the personal information with the registered user is anonymously verifiable by use of an anonymous public key certificate associated with an asymmetric cryptographic public key matching an asymmetric cryptographic private key under the control of a portable storage device of the registered user.

47. The electronic storage of claim 46 wherein the personal information is anonymously indexed by having associated with each item of personal information of the registered user an electronic record pointer, and wherein the anonymous public key certificate contains the electronic record pointer.

48. The electronic storage of claim 46 or claim 47 wherein the anonymous public key certificate contains a personal data component.

49. The electronic storage of claim 48 wherein the personal data component comprises biometric data of the registered user.

50. The electronic storage of any one of claims 46 to 49, wherein the asymmetric cryptographic private key is stored in the portable storage device.

51. The electronic storage of any one of claims 46 to 49, wherein an access code is stored in the portable storage device allowing access to the asymmetric cryptographic private key.

52. The electronic storage of any one of claims 46 to 549, wherein the asymmetric cryptographic private key can be copied with the registered user's authorisation from the portable storage device into the possession of an authorised user.

53. The electronic storage of claim 52 wherein the copied asymmetric cryptographic private key in the possession of the user is caused to be deleted upon occurrence of a predetermined event.

54. The electronic storage of claim 53 wherein the predetermined event is the authorised user entering an update to the indexed personal information of the registered user.

55. The electronic storage of claim 53 wherein the predetermined event is lapsing of an authorisation period.

56. The electronic storage of any one of claims 52 to 55 wherein the authorised user is a health care professional authorised by the registered user to enter an update to the registered user's indexed personal information.

57. A method of issuing Public Key Certificates to Registered Persons within an electronic record system, the method comprising the steps of:

- Issuing on behalf of each Registered Person whose personal information is held within an electronic record system a portable personal computing device with the ability to control the storage of one or more asymmetric cryptographic Private Keys.
- Visibly printing upon the surface of the personal computing device human readable identity information pertaining to the Registered Person.
- Generation of at least one pair of matching asymmetric cryptographic Private and Public Keys.
- Storage of at least one of the asymmetric cryptographic Private Keys under the control of the portable personal computing device.
- Creation on behalf of each Registered Person a Public Key Certificate for each asymmetric cryptographic Public Key which matches each asymmetric cryptographic Private Key stored under the control of the portable personal computing device.

- Inclusion in one or more of the Public Key Certificates one or more electronic record pointers with which personal information pertaining to the Registered Person may be indexed within the electronic record system.
- Issuance of the Public Key Certificate(s) to the Registered Persons.

58. The method according to claim 57 wherein the asymmetric cryptographic Private Key is stored within the portable personal computing device.

59. The method according to claim 57 wherein the asymmetric cryptographic Private Key is stored in an external computer system separate from the portable personal computing device where the external computer system is accessed under the control of the portable personal computing device.

60. The method according to any one of claims 57 to 59 wherein the portable personal computing device is a smartcard.

61. The method according to any one of claims 57 to 60 wherein the Public Key Certificate does not contain the name of the Registered Person to whom the Public Key Certificate has been issued.

62. The method according to any one of claims 57 to 61 wherein the Public Key Certificate does not contain any identity information pertaining to the Registered Person to whom the Public Key Certificate has been issued.

63. The method according to any one of claims 57 to 62 where a plurality of asymmetric cryptographic Private Keys are stored under the control of the portable personal computing device and Public Key Certificates corresponding respectively to different asymmetric cryptographic Private Keys are issued by a plurality of entities.

64. The method according to any one of claims 57 to 63 wherein the portable personal computing devices with associated asymmetric cryptographic Private Key storage are initially distributed without Private Keys being yet stored under the control of the personal computing devices.

65. The method according to any one of claims 57 to 64 wherein Digital Signature codes are created for given data items within the electronic record system in order to

explicitly link each digitally signed data item to the value of an electronic record pointer contained in a Public Key Certificate issued to the Registered Person and associated with the Digital Signature codes.

66. The method according to any one of claims 57 to 65 wherein verification using the Public Key Certificate of a given Digital Signature code for a given data item in the electronic record system is used to evince the association of the data item with an electronic record pointer value contained in the Public Key Certificate.

67. The method according to any one of claims 57 to 66 wherein Digital Signature codes are created for given data items in the electronic record system using an asymmetric cryptographic Private Key issued to the Registered Person where each Digital Signature code is interpreted as explicitly recording the consent of the Registered Person to the creation of each respective digitally signed the data item.

68. The method according to any one of claims 57 to 67 wherein access to an electronic record system is granted to the holder of a portable personal computing device based on the success of an asymmetric cryptographic challenge-response where the challenge utilises the Public Key associated with digitally signed data items contained in the electronic record system and the response utilises a Private Key controlled by the portable personal computing device.

69. The method according to any one of claims 57 to 68 wherein Public Key Certificates associated with one electronic record system are issued corresponding to respective asymmetric cryptographic Private Keys stored under the control of portable personal computing devices issued by a plurality of entities.

70. The method according to any one of claims 57 to 69 wherein the portable personal computing device is a government issued identity card.

71. The method according to any one of claims 57 to 70 wherein the portable personal computing device is a government issued entitlement card.

72. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued by a financial institution to a customer of the financial institution.

73. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued on behalf of a financial institution to a customer of the financial institution.

74. The method according to any one of claims 57 to 71 wherein the portable personal computing device forms part of a government issued travel document.

75. The method according to any one of claims 57 to 71 wherein the portable personal computing device is a vehicle driver license.

76. The method according to any one of claims 57 to 71 wherein the portable personal computing device is a business license.

77. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued by or on behalf of a commercial organisation to one of its customers.

78. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued by or on behalf of an educational institution to a student.

79. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued by or on behalf of an employer to one of its employees.

80. The method according to any one of claims 57 to 69 wherein the portable personal computing device is issued by or on behalf of an association to one of its members.

81. The method according to any one of claims 57 to 69 wherein the portable personal computing device is a subscriber identification module within a mobile telephone.

82. The method according to any one of claims 57 to 69 wherein the portable personal computing device is a subscriber identification token associated with a subscription television set-top box.

83. The method according to any one of claims 57 to 69 wherein the portable personal computing device is a road toll identification device.

84. The method according to any one of claims 57 to 69 wherein the portable personal computing device is a radio frequency identification tag.

85. The method according to any one of claims 57 to 84 wherein the electronic record system is for the purpose of recording votes in an electoral system cast by the Registered Person to whom the portable personal computing device has been issued.

86. The method according to any one of claims 57 to 85 wherein the electronic record system is for the purpose of undertaking commercial transactions with the Registered Person to whom the portable personal computing device has been issued.

87. The method according to any one of claims 57 to 86 wherein the electronic record system is for the purpose of accounting for the movements of the Registered Person to whom the portable personal computing device has been issued.

88. The method according to any one of claims 57 to 87 wherein the electronic record system is an electronic health record system.

89. The method according to any one of claims 57 to 88 wherein the electronic record system is for the purpose of managing customer accounts.

90. The method according to any one of claims 57 to 89 wherein the electronic record system is for the purpose of managing a customer loyalty programme.

91. The method according to any one of claims 57 to 90 wherein the electronic record system holds personal information collected from the Registered Person to whom the portable personal computing device has been issued.

92. A means for issuing Public Key Certificates to Registered Persons within an electronic record system, the means comprising the elements of:

- One or more portable personal computing devices with the ability to control the storage of one or more asymmetric cryptographic Private Keys.
- A recognised authoritative entity to issue the portable personal computing devices to Registered Persons about whom personal information is held within the electronic record system.
- Human readable identity information pertaining to the Registered Persons visibly printed on the surface of respective the portable personal computing devices.
- A key generation system to create at least one pair of asymmetric cryptographic Private and Public Keys for each Registered User.
- A Public Key Certificate issued to each Registered Person corresponding to each asymmetric cryptographic Private Key stored under the control of the portable personal computing devices.
- At least one electronic record pointer contained within the data contents of each Public Key Certificate where the electronic record pointer may be used to index records within the electronic record system pertaining to the Registered Person to whom each Public Key Certificate has been issued.
- A Certification Authority which creates the Public Key Certificates for the Registered Persons.

93. The means according to claim 92 wherein Digital Signature codes created for given data items within the electronic record system are interpreted as explicitly linking each digitally signed data item to the value of an electronic record pointer contained in a Public Key Certificate issued to the Registered Person and associated with the Digital Signature codes.

94. The means according to either of claims 92 or 93 wherein the verification using the Public Key Certificate of a given Digital Signature code for a given data item in the electronic record system is interpreted to evince the association of the data item with an electronic record pointer value contained in the Public Key Certificate.

95. The means according to any one of claims 92 to 94 wherein Digital Signature codes created for given data items in the electronic record system using an asymmetric cryptographic Private Key issued to the Registered Person are interpreted as recording

the consent of the Registered Person to the creation of each respective digitally signed the data item.